Cisco Software-Defined Access

Cisco Secure Enterprise

Jason Gooley, CCIE® x2 (RS & SP) No. 38759
Roddie Hasan, CCIE® RS No. 7472
Srilatha Vemula, CCIE® SEC No. 33670

ciscopress.com

Cisco Software-Defined Access

Jason Gooley, CCIE No. 38759
Roddie Hasan, CCIE No. 7472
Srilatha Vemula, CCIE No. 33670

Cisco Press

Note As of Cisco DNA Center version 1.3, LAN Automation discovers devices up to two layers deep below the seed device.

The LAN Automation process consists of two phases. The first phase begins when the user inputs the required information on the LAN Automation screen and clicks Start. During the first phase, a temporary configuration is applied to the seed device to facilitate the PnP process and then the initial discovery of new devices in the network begins. The length of time that this process takes depends on the network speed and number of new devices to be discovered and configured, but you should expect it to take a minimum of ten minutes to discover and initially configure all new devices.

Figure 4-4 shows the first phase of LAN Automation with three devices discovered and in a Completed state. The process remains in this state until it is stopped.

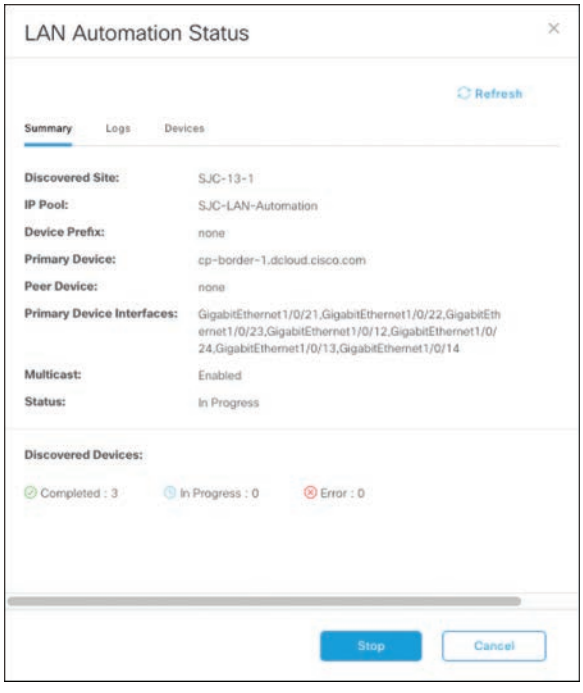

Figure 4-4 *LAN Automation Status During Phase One*

Note Because Cisco DNA Center does not know the exact number of devices that will be discovered, the first phase of LAN Automation runs indefinitely until you click Stop in the LAN Automation Status dialog box, which you should do after the number of expected network devices are discovered. This action automatically starts phase two of the LAN Automation process.

During phase two, a final configuration based on the site's network settings is applied to the new devices, including a software upgrade and reload, if required. The temporary configuration applied in phase one is also removed from the seed device. Again, the length of this process depends on the number of newly discovered devices but typically takes a minimum of ten minutes to complete. Once this phase is complete, the LAN Automation process automatically ends and all newly discovered devices are placed in the Cisco DNA Center Inventory and fully configured to be part of the Cisco SD-Access underlay.

Figure 4-5 shows a fully completed LAN Automation Status screen with three devices discovered and fully onboarded. Note that the status shows as Completed.

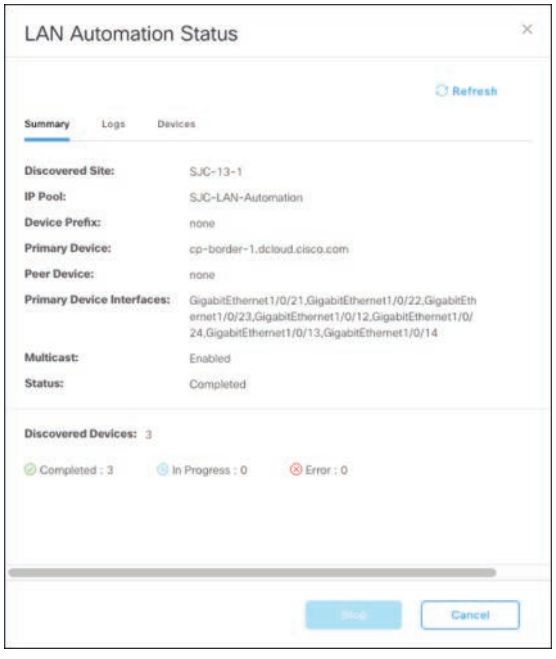

Figure 4-5 *LAN Automation Status Completed Screen*

Example 4-2 is a configuration excerpt following a successful LAN Automation process showing the configuration that is pushed to the newly onboarded switches.

Example 4-2 *Excerpt from Sample LAN Automation Configuration*

```
interface Loopback0
 description Fabric Node Router ID
 ip address 100.124.128.141 255.255.255.255
 ip pim sparse-mode
 ip router isis
 clns mtu 1400
!
```

```
interface GigabitEthernet1/0/21
 description Fabric Physical Link
 no switchport
 dampening
 ip address 100.124.128.148 255.255.255.254
 ip pim sparse-mode
 ip router isis
 ip lisp source-locator Loopback0
 load-interval 30
 bfd interval 100 min_rx 100 multiplier 3
 no bfd echo
 clns mtu 1400
 isis network point-to-point
!
interface GigabitEthernet1/0/22
 description Fabric Physical Link
 no switchport
 dampening
 ip address 100.124.128.146 255.255.255.254
 ip pim sparse-mode
 ip router isis
 ip lisp source-locator Loopback0
 load-interval 30
 bfd interval 100 min_rx 100 multiplier 3
 no bfd echo
 clns mtu 1400
 isis network point-to-point
!
router isis
 net 49.0000.1001.2412.8141.00
 domain-password cisco
 metric-style wide
 log-adjacency-changes
 nsf ietf
 bfd all-interfaces
```

Figure 4-6 shows the Cisco DNA Center Inventory tool with the newly discovered and onboarded devices assigned to the site.

Figure 4-6 *Cisco DNA Center Inventory Following LAN Automation*

Wireless LAN Controllers and Access Points in Cisco Software-Defined Access

The Cisco Wireless LAN Controller (WLC) plays a special role in a Cisco SD-Access network, as it physically lives outside of the fabric underlay yet still provides control channel capabilities to fabric-enabled access points (APs) and service set identifiers (SSIDs).

Note The exception to this is the Cisco Catalyst 9800 Embedded Wireless feature that is available for the Cisco Catalyst 9300, 9400, and 9500 Series Switch platforms. This feature supports only fabric-enabled SSIDs and runs on switches inside the fabric.

Fabric-enabled access points connect to fabric edge switches and use the underlay to establish a Control and Provisioning of Wireless Access Points (CAPWAP) tunnel with the WLC. This tunnel carries control channel information, including wireless host reachability information, from the APs to the WLC, which is in turn advertised to the fabric control plane node in the fabric. AP connectivity in Cisco SD-Access is discussed further in Chapter 5, "Cisco Identity Services Engine with Cisco DNA Center."

Figure 4-7 shows a typical Cisco SD-Access topology with WLC placement outside of the fabric and wireless access points connecting to fabric edge nodes.

Data plane (or endpoint) traffic is sent directly from the AP to the fabric edge switch so that traffic stays local to the fabric, where it is subject to the same policy and flow as applied to wired endpoint traffic. This also increases the efficiency and performance of wired-to-wireless communication, because wireless traffic is no longer centralized at the WLC as it is in traditional wireless environments.

Fabric access points and WLCs can also run in hybrid configurations, supporting both fabric-enabled SSIDs and traditional centralized SSIDs on the same hardware. This setup is useful for migration scenarios where legacy SSIDs are still required for a set of clients. Provisioning of non-fabric SSIDs in Cisco DNA Center is discussed in Chapter 3.

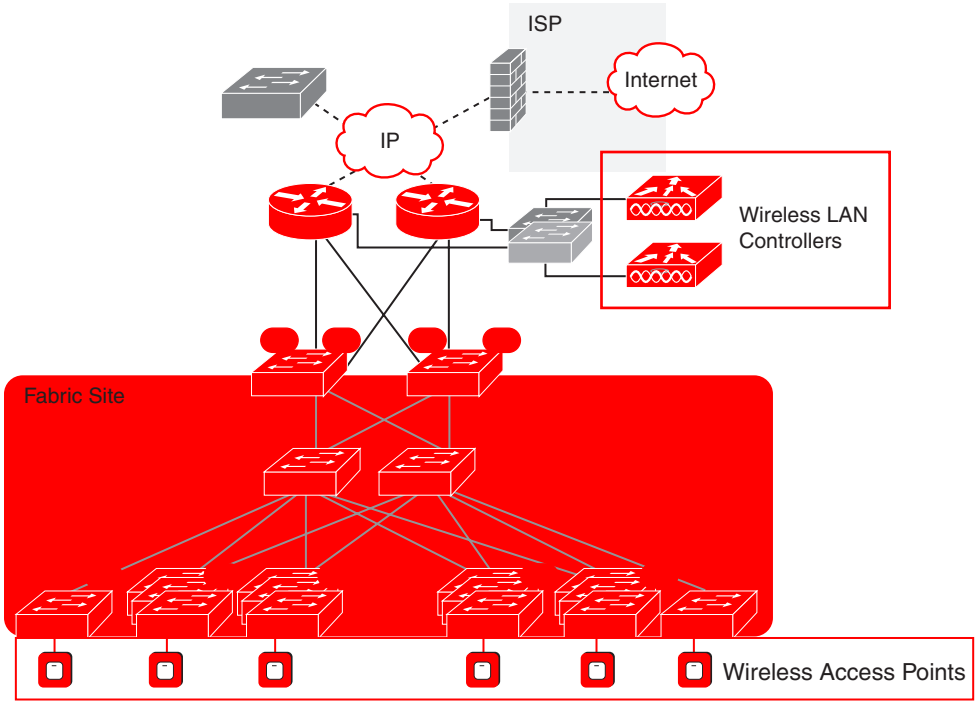

Figure 4-7 *Cisco SD-Access Topology with Wireless Infrastructure*

Shared Services

Shared services in a Cisco SD-Access environment are any services that are common to the enterprise and typically live outside of the Cisco SD-Access fabric but still need to communicate with hosts in the fabric on all virtual networks (VNs). Some common examples of shared services are

- **Dynamic Host Configuration Protocol (DHCP):** Provides IP addresses and other settings to hosts on a network using a centralized database
- **Domain Name System (DNS):** Provides name-resolution services to hosts in a network
- **Network Time Protocol (NTP):** Provides accurate time information for hosts and network devices to synchronize their system clocks

Figure 4-8 is an example of shared services placement in a typical enterprise. These services are in the data center and outside of the Cisco SD-Access fabric.

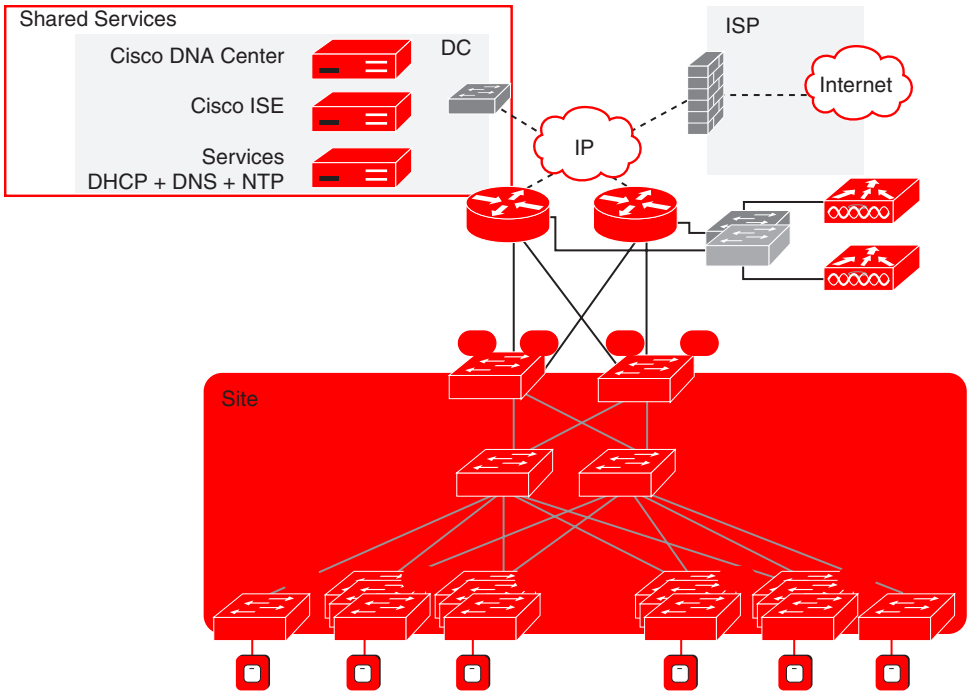

Figure 4-8 *Shared Services in a Cisco Software-Defined Access Topology*

Shared services typically need to be reachable from all networks, including the underlay, so an intermediate device or connection point is required outside the fabric to facilitate these connections. Cisco SD-Access uses the concept of a *fusion router* for this purpose, which lives outside of the fabric and is connected directly to the border node(s). The fusion router is discussed later in this chapter.

Transit Networks

Transit (or peer) networks in Cisco SD-Access define the type of networks that exist outside of the fabric and that are connected to the fabric border node(s). The actual network medium could be a WAN in the case of a branch, or a data center LAN connection in the case of a large campus. Regardless of the medium, there are two types of transits that can be defined with Cisco SD-Access: IP-Based and SD-Access.

IP-Based Transit

IP-Based transits provide traditional IP connectivity from the outside world to the fabric and vice versa. To maintain macro-segmentation outside of the fabric, the connections should use VRF-lite for traffic separation. Traffic is typically routed from the border to the transit next-hop router using external Border Gateway Protocol (eBGP), but any routing protocol can be used so long as it is VRF-aware, as next-hop peers are needed across each of the VNs/VRFs as well as the underlay.